LESSONS TO LEARN FROM ATTACKS ON COVID-19 RESEARCH

With COVID-19 creating the challenges that it has for so many, there is little wonder that creating a vaccine is such a major focus. Unfortunately, hackers are aware of this focus, and how it makes the organizations conducting vaccine trials particularly vulnerable. Let's examine this situation, and the lessons that all businesses can take away from it.

COZY BEAR

The National Cyber Security Centre, located in the UK, recently shared that a group has been attacking organizations involved with COVID-19 vaccine research. These claims have been verified by authorities in the United States and Canada.

Known as "APT29," as well as "Cozy Bear" and "the Dukes," the attackers level spear phishing attacks and make use of assorted exploits to gain access to their target's systems. After this access has been obtained, malware known as WellMail or WellMess is released into the environment. Many experts are of the opinion that this is not the first time that APT29 has been active, either. The group is suspected of attacks against various organizations in healthcare, energy, and government, and is believed to be responsible for the 2016 hack of the Democratic National Committee.

In response to this, the CSC has been trying to work with software vendors to ensure that vulnerabilities are patched. If these patches aren't applied, cybercriminals can find the means to exploit these vulnerabilities and cause problems.

A SPEAR PHISHING REFRESHER

We're no strangers to discussions about phishing, simply because it is one of today's most prevalent threats to network security. Many phishing attacks are sent randomly to a large group of targets, but spear phishing is a different animal. Instead of trying to exploit a lot of people for little payout from each, spear phishing requires careful planning and execution of a highly targeted attack against one person. This person is often seen as the weakest link in an organization's security by hackers.

With any luck, you won't need to contend with phishing attacks from a major hacking group. That being said, it's important that you and your team can identify a potential phishing attack and react appropriately. Here are a few basics to keep in mind:

- Always check the details. Many phishing attacks will display some subtle issue, either in the email address it comes from or some other detail. Make sure you pay attention for some of these warning signs.
- Proofread the message. Businesses want to put their best foot forward, so their correspondence is generally carefully edited before it's sent out. If you receive a message with questionable spelling and grammar, exercise caution.
- Reach out. If you're unsure of whether a message is legitimate or not, reach out to the sender through another means to confirm it if you can.

For your business to avoid threats, being able to identify potential phishing attacks is only going to become more important. Find out how to train your team to spot them by reaching out to us. Call eb Logix, Inc at 610.813.4900 and visit www.eblogix.com to learn more.

The Top Three Reasons Clients Choose eb Logix:

eb Logix President Courtney Briddes

WE KEEP IT SIMPLE.

We understand that technology is a vital component but may not be the primary focus of your business. Our team is able to communicate technology solutions at a level that is easy to understand so you can focus on your business goals.

WE KEEP IT SMART.

Our team has a wealth of knowledge in the IT field to provide you with the best technology solutions. We can assess and resolve everyday technology issues, provide long term technology plans, and also manage large infrastructure projects.

WE KEEP IT SECURE.

Cyber criminals are becoming more sophisticated every year. It's a very real threat and the largest area of concern for businesses today. We take your company's security seriously and partner with some of the best security manufacturers in the industry.

eb LOGIX
Your IT Solution
simple. smart. secure.